Anlage SUB – Unterauftragnehmer, externe Dienste und Drittlandtransfers

Sentinel System / Virtueller Bürger-Schreibtisch / Schuldnerberatung

Version 1.0 · Stand 09.10.2026

Arbeitsfassung: Anbieterstatus und Drittlandtransfers sind funktionsbezogen zu prüfen. Technische Unterstützung allein begründet keine Einordnung als Unterauftragnehmer.

1. Zweck

Diese Anlage dokumentiert externe Anbieter und technische Dienste, die bei der Bereitstellung von Sentinel System beziehungsweise des Virtuellen Bürger-Schreibtischs personenbezogene Daten im Auftrag verarbeiten können.

Dabei wird zwischen drei Kategorien unterschieden:

- AKTIV – Bestandteil des derzeitigen produktiven Betriebs.
- OPTIONAL – nur bei Aktivierung einer bestimmten Funktion relevant.
- ZU VERIFIZIEREN – technischer beziehungsweise vertraglicher Datenfluss muss vor Aufnahme in die veröffentlichte Liste abschließend geprüft werden.

Ein Anbieter wird nicht allein deshalb als Unterauftragnehmer bezeichnet, weil dessen Software oder Schnittstelle technisch unterstützt wird.

2. Hetzner – Hosting

Der Virtuelle Bürger-Schreibtisch wird gegenwärtig auf Hetzner-Infrastruktur in Nürnberg betrieben.

Dabei können insbesondere Kontodaten, Dokumente, Metadaten, Schuldnerberatungsdaten und technische Betriebsdaten auf der Infrastruktur verarbeitet werden.

Merkmal	Stand
Anbieter	Hetzner
Funktion	Hosting / Serverinfrastruktur
Status	AKTIV
Einsatz	Sentinel System und Virtueller Bürger-Schreibtisch
Standort	Nürnberg, Deutschland
Daten	abhängig vom jeweiligen Sentinel-Dienst
Bürgerdokumente möglich	Ja
Drittlandtransfer	nach derzeitigem Bereitstellungsmodell nicht erforderlich
AV-Einbindung	vor Veröffentlichung Vertragsunterlagen/AVV dokumentieren

Status: AKTIV

Offener Prüfpunkt: Vertragsunterlagen und AVV vor verbindlicher Veröffentlichung dokumentieren.

3. Lokale OCR- und Dokumentenverarbeitung

OCR und Dokumentenkonvertierung sind nach der dokumentierten Sentinel-Architektur innerhalb der eigenen Anwendungsinfrastruktur möglich.

Hierfür werden insbesondere lokale Komponenten eingesetzt beziehungsweise vorgesehen, beispielsweise Tesseract und LibreOffice.

Eine normale OCR- oder Office-Konvertierung erfordert nicht allein aufgrund dieser Funktion die Übermittlung des Bürgerdokuments an einen externen Cloud-OCR-Anbieter.

Diese Komponenten sind deshalb keine externen Unterauftragnehmer.

Status: INTERN

4. Externe KI-Dienste

Externe KI-Funktionen existieren beziehungsweise sind innerhalb der Sentinel-Welt vorgesehen. Die Datenflüsse unterscheiden sich je nach Produkt und Funktion erheblich.

Jede externe KI-Verarbeitung erhält deshalb vor Produktivfreigabe einen eigenen Datensatz.

Prüfpunkt	Erforderlich
Anbieter	festzustellen
konkrete KI-Funktion	festzustellen
übermittelte Daten	festzustellen
personenbezogene Daten	Ja/Nein
Dokumentinhalt	Ja/Nein
Speicherfrist Anbieter	prüfen
Training mit Eingaben	prüfen
EU-Verarbeitung	prüfen
Drittlandtransfer	prüfen
AVV/DPA	prüfen
Transfermechanismus	falls erforderlich
Abschaltbarkeit	dokumentieren

Eine pauschale Aussage, externe KI erhalte keine personenbezogenen Daten, wird nur getroffen, wenn dies für jede entsprechende Funktion tatsächlich belegt ist.

Status: ZU VERIFIZIEREN

5. KI-Recherche des Bürger-Schreibtischs

Für den Recherche-Executor des Bürger-Schreibtischs existiert ein enger technischer Datenvertrag.

Nicht übertragen werden sollen insbesondere:

- Bürgerdokumente
- Aktenzeichen
- private Bürgernotizen
- account_id
- user_id
- matter_id

Übermittelt werden dürfen nur die für die ausdrücklich ausgelöste öffentliche Recherche erforderlichen, minimierten Suchparameter.

Das Ergebnis wird als Vorschlag zurückgegeben und vor einer Übernahme in gemeinsame Datenbestände menschlich geprüft.

Status: Datenschutzkonzept: UMGESETZT/DOKUMENTIERT; externer Anbieter und tatsächlicher Transportweg: ZU VERIFIZIEREN

6. Web Speech API / Sprachfunktionen

Browser-Sprachfunktionen können abhängig von Browser, Betriebssystem und verwendetem Speech-Service technisch unterschiedlich verarbeitet werden.

Eine ausschließlich lokale Spracherkennung wird deshalb nicht pauschal zugesichert.

Vor produktiver Aktivierung wird der Datenfluss dokumentiert:

Browserfunktion → Sprachdaten → möglicher externer Anbieter → Speicher-/Transferbedingungen

Status: OPTIONAL / ZU VERIFIZIEREN

7. eBO / EGVP / SAFE

Diese Dienste sind nicht automatisch Unterauftragnehmer von Sentinel, nur weil Sentinel mit ihnen kommuniziert.

Zu unterscheiden sind technische Kommunikationsinfrastruktur und Auftragsverarbeitung für Sentinel.

SAFE-/eBO-/EGVP-Kommunikation wird deshalb in der Datenflussdokumentation geführt, aber nicht ohne rechtliche Prüfung als klassischer Unterauftragnehmer bezeichnet.

Status: EXTERNER KOMMUNIKATIONSEMPFÄNGER/-DIENST

8. E-Mail-Infrastruktur

Sentinel kann E-Mail-Funktionen bereitstellen beziehungsweise fremde Mailkonten anbinden.

Zu unterscheiden sind eine Sentinel-eigene Mailbox und ein vom Nutzer eingebundener externer Mailprovider.

Ein vom Bürger selbst eingebundener Mailanbieter ist nicht automatisch Unterauftragnehmer von Sentinel.

Soweit Sentinel selbst Mailinfrastruktur bei einem externen Provider bezieht, wird dieser entsprechend der tatsächlichen Vertragsstruktur geprüft und gegebenenfalls in die Unterauftragnehmerliste aufgenommen.

Status: ZU VERIFIZIEREN

9. Messenger und Cloud-Laufwerke

Eine technisch vorhandene Schnittstelle führt nicht automatisch zu einer Datenübertragung.

Erst wenn ein Nutzer einen entsprechenden Dienst verbindet beziehungsweise eine Übertragung auslöst, entsteht der konkrete Datenfluss.

Für jeden unterstützten Dienst wird separat dokumentiert:

Anbieter → Authentisierung → Datenumfang → Richtung → Speicherort → Rolle → Drittlandtransfer

Status: OPTIONAL

10. Zahlungsdienstleister

Soweit kostenpflichtige Sentinel-Angebote Zahlungsdienstleister einsetzen, können dort insbesondere Zahlungs- und Abrechnungsdaten verarbeitet werden.

Für einen kommunalen Pilot wird geprüft, ob ein Zahlungsdienst überhaupt Bestandteil des Pilotdatenflusses ist. Ist dies nicht der Fall, wird er nicht unnötig in die produktspezifische Pilot-Unterauftragnehmerliste aufgenommen.

Status: PILOTABHÄNGIG

11. DNS, Domain und TLS

Domainregistrare, DNS-Anbieter und Zertifizierungsstellen sind gesondert zu betrachten. Sie verarbeiten nicht automatisch Bürgerdokumente des Systems.

Mögliche Daten beschränken sich abhängig von der Architektur beispielsweise auf IP-Adressen, Domaininformationen, DNS-Anfragen und Zertifikatsmetadaten.

Die Einordnung erfolgt nach dem tatsächlichen technischen Datenfluss.

Status: ZU VERIFIZIEREN

12. Monitoring und Fehleranalyse

Externe Monitoring-, Crash-Reporting- oder Analytics-Dienste sind vor Produktivbetrieb zwingend zu erfassen.

Besonders kritisch wären URLs mit Objektkennungen, Benutzerkennungen, Dokumentnamen, Stacktraces mit Inhaltsdaten oder Sessioninformationen.

Monitoringdaten werden als eigener Datenfluss behandelt und dürfen nicht ungeprüft personenbezogene Fachinhalte an externe Systeme übertragen.

Status: ZU VERIFIZIEREN

13. Derzeitige Pilotmatrix

Für einen ersten Bürger-Schreibtisch-Pilot wird konservativ nur der derzeit belegbare Status veröffentlicht.

Hetzner	Server-/Hostinginfrastruktur	AKTIV	Deutschland
lokale OCR	Dokumentenerkennung	INTERN	–
lokale Dokumentkonvertierung	Office/PDF-Verarbeitung	INTERN	–
externe KI	optionale KI-Funktionen	vor Pilot zu spezifizieren	prüfen
Recherche-Executor	öffentliche Recherche	OPTIONAL	Anbieter prüfen
eBO/SAFE	sichere Kommunikation	OPTIONAL	gesonderter Kommunikationsweg
externe Mailanbieter	Nutzerintegration	OPTIONAL	anbieterspezifisch
Messenger/Drives	spätere Integration	OPTIONAL	anbieterspezifisch

Die Matrix behauptet an keiner Stelle mehr, als derzeit technisch belegt werden kann.

14. Drittlandgrundsatz

Dazu gehören abhängig vom Empfänger insbesondere:

- Angemessenheitsbeschluss
- geeignete Garantien
- Standardvertragsklauseln
- gegebenenfalls Transfer Impact Assessment
- ergänzende technische Maßnahmen

Die Aktivierung eines externen Dienstes mit Übermittlung personenbezogener Daten außerhalb des EU-/EWR-Raums erfolgt erst nach dokumentierter Prüfung der datenschutzrechtlichen Voraussetzungen.

Ein externer Dienst wird nicht allein deshalb als datenschutzrechtlich unproblematisch behandelt, weil seine API verschlüsselt über HTTPS erreichbar ist.

15. Änderungen der Unterauftragnehmer

Der Auftragnehmer informiert den Auftraggeber über beabsichtigte Änderungen hinsichtlich der Hinzuziehung oder Ersetzung weiterer Auftragsverarbeiter entsprechend der vereinbarten Informationsfrist.

Dem Auftraggeber wird Gelegenheit gegeben, aus datenschutzrechtlich nachvollziehbaren Gründen Einwände gegen die Änderung zu erheben.

Offener Prüfpunkt: Die konkrete Informationsfrist wird im jeweiligen AVV festgelegt; 30 Tage sind lediglich ein Arbeitsvorschlag.

16. Öffentliche Darstellung

Öffentlich werden keine unnötigen internen Details, Ports oder Sicherheitsmechanismen ausgebreitet.

Die öffentliche Zusammenfassung umfasst insbesondere:

- Hosting: Deutschland
- Dokumentenverarbeitung: lokale Verarbeitung, soweit technisch vorgesehen
- Externe KI: nur funktionsbezogen und transparent dokumentiert
- Unterauftragnehmer: aktuelle Liste abrufbar
- Drittlandtransfers: nur unter den Voraussetzungen der DSGVO

Eine vollständige vertrags- und pilotspezifische technische Anlage wird dem Datenschutzbeauftragten beziehungsweise Vertragspartner bereitgestellt.